

Technische Aspekte 1: Netzwerkübertragung und Zertifikate

Eine zentrale Strategie von Phishing-Angriffen ist es, dich auf manipulierte Webseiten zu schicken, damit du dort deine sensiblen Daten eingibst und sie damit dem Betrüger unbemerkt überlässt. Um dich vor unsicheren Webseiten zu bewahren, verfügen viele Internet-Browser über Schutzfunktionen:

A.1 – Öffne die folgende Webseite und beobachte deinen Browser.

Beschreibe, wie dein Browser dich vor ihr warnt. (Du musst das Quiz nicht bearbeiten)



<http://www.paul-orzessek.de/einbuengerungstest/test.htm>

Doch woran erkennt dein Browser das? Das kann er u.a. an dem Beginn der URL erkennen. Das hängt damit zusammen, wie die Webseiten-Daten versendet werden.

Hintergrund: HTTP und Netzwerkübertragung

Jede Webseiten-Adresse beginnt mit **http**. Das steht für *Hypertext Transfer Protocol* und beschreibt den Standard im Internet zur Übertragung von Daten. Es regelt, wie und in welcher Form dein Browser die Daten der Webseiten (Aufbau und Inhalt) von einem Server anfordert und erhält und zurücksendet.

Hier ist ein beispielhafter Datenaustausch, den ein Browser an einen Server sendet:

```
GET /login http/1.1
Host: www.meine-bank.com
Accept: text/html, application/xml
Accept-Language: de-DE, en-us
Accept-Encoding: gzip, deflate
User-Agent: Mozilla/5.0
Content-Length: 85
Cookie: sitzung=76bjvj45hjb
Connection: keep-alive

Csrf_token=ks729dQ786UnH133wZ&user=peter.schmidt&
password=Liebel23!&stay_logged_in=on
```

A.2 – Nenne drei Informationen, die du aus dieser Datenübertragung erkennen kannst, und **beschreibe** kurz, was sie bedeuten.

1. _____
2. _____
3. _____

A.3 – Welche der Informationen könnte für einen Betrüger wertvoll sein? Begründe.

Man-in-the-Middle-Angriffe

Standard-HTTP besitzt eine zentrale Schwäche: Alle Daten werden im **Klartext** übertragen. Sie sind also durch den Menschen lesbar. Auf dem Weg zwischen deinem Gerät und dem Server gehen die Daten durch viele Zwischenstationen – WLAN, Router, Netze – die alle das HTTP mitlesen können.

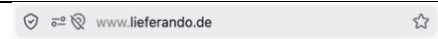
Diese Schwäche können sich Betrüger*innen zunutze machen. Bei sogenannten **Man-in-the-Middle-Angriffen** („Mann in der Mitte“) schaltet sich ein Angreifer zwischen dich und einen Server. Dabei kann er die Daten nicht nur **mitlesen**, sondern auch unterwegs verändern, ohne dass du oder der Server es merken.

A.4 – Beschreibe, warum dein Browser Webseiten, welche die Daten über Standard-HTTP übertragen, als „nicht sicher“ markiert.

HTTPS

Um diese Art des Angriffes zu verhindern, wird heutzutage meist eine erweiterte Form des Standard-HTTP verwendet: **https**. Das „s“ steht für „Secure“ und bedeutet, dass die Datenübertragung verschlüsselt ist. Ein*e Mitleser*in sieht statt des Klartextes eine komplexe, unlesbare Zeichenkette. Gute Verschlüsselungen sind stark, sodass sich der Klartext auch mit viel Rechenleistung von Unbefugten praktisch nicht wiederherstellen lässt. Ob eine Webseite verschlüsselt ist, wird dir in deinem Browser auch durch ein Symbol angezeigt.

A.5 – Gebe an, ob die Webseite der gegebenen URLs verschlüsselt sind.

URL	verschlüsselt	Nicht verschlüsselt
http://www.telekon.net/tarife/internet-tarife-young	☐	☐
https:// https://www.duden.de/schreibassistent	☐	☐
	☐	☐
	☐	☐

A.6 – Erkläre, warum die Eingabe von sensiblen Daten bei Seiten mit *https://* sicherer ist als bei Seiten mit einfachem *http://*.

Jedoch gibt es hierbei ein Problem: Eine verschlüsselte Netzwerkkommunikation kann nicht nur bei seriösen, sondern auch bei betrügerischen Webseiten eingerichtet sein. Zwar können Man-in-the-Middle-Angriffe verhindert werden, jedoch bringt das nichts, wenn die Webseite an sich von einem Phisher ist, der sich z.B. als deine Bank ausgibt.

Um sicherzugehen, ob eine Seite sicher ist, benötigt man nicht nur einen Beweis dafür, ob sondern auch **mit wem** man verschlüsselt kommuniziert. Hierfür gibt es eine Lösung:

Digitale Zertifikate

Digitale Zertifikate (auch SSL-Zertifikate) dienen dazu, die Identität von Personen oder Organisationen im Internet zu bestätigen und eine sichere Verbindung zu ermöglichen. Sie sind eine Art „digitaler Ausweis“ für eine Webseite. Es beinhaltet verschiedene Informationen:

- Informationen über den Inhaber
- Öffentlicher Schlüssel (dient der Verschlüsselung)
- Gültigkeitsdauer
- Signatur einer Zertifizierungsstelle

Ein SSL-Zertifikat wird von einer von der Webseite unabhängigen Zertifizierungsstelle ausgestellt und signiert. Browser kennen vertrauenswürdige Zertifizierungsstellen und kontrollieren deren Siegel. Wenn das Siegel nicht bekannt ist oder die Domain¹ der Webseite nicht zum Zertifikat passt, stellt der Browser eine Warnung aus oder bricht die Verbindung ab.

¹ Eine Domain ist der menschenlesbare Name eines Servers und für eine Webseite die „Hauptadresse“. Für mehr Informationen siehe „Warnung 4: Domain-Spoofing“ (S.1) oder recherchiere selbst.

Potenzielle Betrüger*innen können kein gültiges Zertifikat für eine bestehende fremde Domain erhalten, weil Zertifizierungsstellen prüfen, ob der Antragssteller diese wirklich besitzt.

Ein Zertifikat gilt für alle Unterwebseiten und Subdomains einer Domain:

(z.B. google.com und google.com/login und mail.google.com)

Du kannst dir diese im Browser anzeigen lassen. Das geht z.B. bei Firefox so:

Klicke auf  → Verbindung sicher → Mehr Webseiten-Informationen → Zertifikat anzeigen

A.7 – Öffne die Webseite www.paypal.com und betrachte dessen Zertifikat.

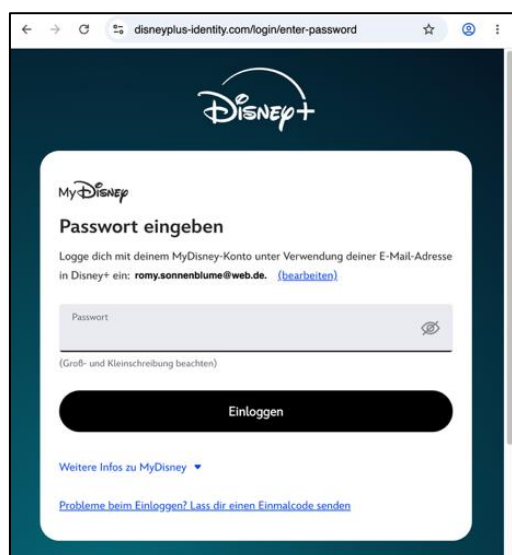
Gebe folgende Informationen aus dem Zertifikat **an**. **Nenne** zwei weitere relevante Informationen aus dem Zertifikat.

Name der Domain	
Name des Inhabers	
Ende der Gültigkeit	
Name der Zertifizierungsstelle	
Weitere Informationen	

Zertifikate ermöglichen es, die Echtheit einer Webseite zu überprüfen:

Szenario

Romy hat einen Link zu einer Seite bekommen, um sich zu verifizieren. Sie ist sich der Gefahr von Phishing bewusst und unsicher, ob sie der Webseite vertrauen kann. Um die Echtheit zu prüfen, öffnet sie das SSL-Zertifikat der Seite.



A.8 – Begründe, ob Romy der Webseite vertrauen kann.

(Tipp: Wenn du dir bei einer Seite unsicher bist, kannst du das Zertifikat mit dir bekannten Webseiten des Unternehmens vergleichen.)

Große Organisationen betreiben häufig mehrere Webseiten unter verschiedenen Namen. Statt für jede Webseite ein eigenes Zertifikat ausstellen zu lassen, werden daher oft mehrere Domains in einem Zertifikat zusammengefasst. Lass uns das überprüfen:

A.9 – Öffne die Webseite www.youtube.com und betrachte dessen Zertifikat. **Gebe an**, welche Hauptdomain genannt wird. **Nenne** zwei weitere Domains aus dem Zertifikat.

Hauptdomain und SAN

Ein Zertifikat kann für mehrere Webseiten (bzw. Domains) gleichzeitig gültig sein. Dabei hat jedes Zertifikat eine Hauptdomain (auch *Inhabername* oder Common Name). Zusätzlich kann es eine Liste weiterer gültiger Domains beinhalten. Diese weiteren Domains nennt man auch **SAN** („**S**ubject **A**lternative **N**ames“).

A.10 – Wie kann der Fakt, dass ein Zertifikat alternative Webseiten-Namen eines Unternehmens beinhaltet, uns dabei helfen, eine unbekannte Webseite zu verifizieren? **Notiere** eine **Vermutung**.

A.11 – Begründe, ob du den folgenden URLs vertrauen kannst. Wende dafür folgendes Schema an:

1. Überlege, zu welcher Hauptdomain sie gehören könnte.
2. Öffne die Hauptdomain und öffne das Zertifikat.
3. Prüfe, ob die Domain in der SAN-Liste genannt wird:
 - Ja: Du kannst ihr vermutlich vertrauen.
 - Nein: Du kannst ihr vermutlich nicht vertrauen

Domain	Hauptdomain	Vertrauen (ja/ nein)	Begründung
youtubekids.com	<i>google.com</i>	<i>Ja</i>	<i>Die URL wird als alternative Webseite benannt.</i>
youtubeadults.com			
messenger.com			
paypal-bezahlen.com			

Achtung

Auch wenn diese Methode dabei helfen kann, fragliche Webseiten zu verifizieren, so gilt dies nicht notwendig umgekehrt. Nur weil eine Domain nicht in der SAN-Liste steht, bedeutet das nicht, dass man ihr nicht vertrauen kann.

Manche Unternehmen haben für jeden Service ein separates Zertifikat:

Beispiel Meta Platforms: instagram.com und whatsapp.com haben eigene Zertifikate

Maßnahme

A.12 – Erkläre, inwieweit dir dieses Modul bei der Erkennung von Phishing geholfen hat. Worauf sollte man bei der Beurteilung von E-Mails bzw. Webseiten achten und warum?
